Conceptualising cybersecurity risk of fintech firms and banks sustainability

NAJAF, Khakan, SCHINCKUS, Christophe, MOSTAFIZ, Md Imtiaz and NAJAF, Rabia

Conceptualising cybersecurity risk of fintech firms and banks sustainability

Khakan Najaf*
Taylor's University
No 1. Jalan Taylor's
47500 Subang Jaya, Selangor
Malaysia.
Email: khakannajaf@sd.taylors.edu.my

Christophe Schinckus
Taylor's University
No 1. Jalan Taylor's
47500 Subang Jaya, Selangor
Malaysia.
Email: christophe.schinckus@taylors.edu.my

Md Imtiaz Mostafiz
Sheffield Hallam University
Howard St, Sheffield S1 1WB
United Kingdom
Email: i.mostafiz@shu.ac.uk

Rabia Najaf
Taylor's University
No 1. Jalan Taylor's
47500 Subang Jaya, Selangor
Malaysia.
Email: Rabianaajf@gmail.com

Abstract

Traditional banks are replete with conventional financial mechanisms is being subjected to enormous pressure to minimise costs in a sustainable way. For instance, offering low-interest rates, which squeeze the overall margin. Due to the high demand for a tailored portfolio of products, the availability of sophisticated communication and advance transaction mechanisms lead to an emergence of new types of firms known as financial technology service (i.e., fintech). Recently, the collaboration between these fintech organisations and banks has increased to lessen the bureaucracy and provide fine-tuned service to the consumer. Albeit, such collaboration has increased the cybersecurity risk for both fintech firms and conventional banks. Prior research has scant to acknowledge the cybersecurity risk and the sustainability of these fintech-bank collaborations. Hence, the dilemma is whether the bank should pursue such collaboration to resuscitate the profit margin; or be pragmatic and shirk to eliminate sustainability risk. We propound that the cybersecurity risk is much higher after the collaboration happens in banks. Types of cybersecurity risks are highlighted, and a theoretical model has been developed. We propose that if both fintech and the conventional banks collaboratively abate these cybersecurity risks, then yielding the profitability is much convenient.

Keywords: financial technology, bureaucracy, cybersecurity, fintech.

1. Introduction

Technological advancement, digitalization and globalisation not only benefit countries, companies, and potential stakeholders but also invigorate a growing community of hackers to take advantage of the same advancement in the tech world at a rapid pace. Financial institutions take a major shift (e.g. fintech sandbox) from last decades due to this technological innovation (Haupert, Maier, & Tilo, 2017). In some cases, innovation runs ahead of the development of security (Arakji & Lang, 2007). Fintech sandbox stimulus innovation and collaboration, and allows the traditional banks and fintech players to experience innovative products and services in a live environment jointly (Sajtos & Tőrös, 2018). The prior study suggests that traditional banks become more vulnerable towards the cyber-breaches after collaboration with the fintech firms (Creado & Ramteke, 2020; Mok & Saha, 2017). The reason for high susceptibility of cybersecurity is due to inherent fintech firms' data integrity risk, data leakage risk, and malware attacks (Buckley, Arner, Zetzsche, & Selga, 2019). Consequently, the continuous cyberattacks will result in the theft of valuable and sensitive information, hacking, insider threat, ransomware, and phishing for the banks. It creates a dilemma and questions the partnerships among traditional banks and fintech firms.

The impact of cybersecurity risk of financial technology is economically significant for the financial institutions. We can understand the economic importance of cybersecurity from a recent report, which informs that almost every year $100 billion USD and 508,000 jobs are lost within US wholly because of cyber-attacks (McAfee, 2020). The cybersecurity risk of fintech firms has vast economic implications for the sustainability of traditional banks. The fundamental underpinning of the long-term economic development depends upon the financial institution to take less cyber-risk in the pursuit of stable profitable opportunities. The financial inclusion stimulated by fintech firms is an example of a negative response between fintech firms and economic development. The fintech collaborated banks are trying to achieve economies of scope with the combination of financial services with other services such as big data analytics and sharing-economy businesses for the value-addition of the economy; however, the threats of cybersecurity inhibit these banks to take such actions. Hence, understanding the ultimate impact of cybersecurity risk of fintech firms on financial institutions will facilitate the policymakers to identify channels via which policy adjustments strength the economic welfare.

The findings of this study have both academic and practical implications. This study contributes to the academic literature by highlighting a new phenomenon of the cybersecurity risk of commercial banks after the fintech firms' collaboration. This study suggests the existence of a sandbox will lead to excessive cybercrimes. Given the practical implications, it may be rational to reconsider the fintech collaboration by commercial banks, also banks should build their own cyber-security block. Our findings show that the impact of the fintech collaboration immune to the country-level effect and all the bank-fintech collaborated firms face the cyber-attacks. Thus, this study implies that regulatory authorities should revise the fintech sandbox system.

The rest of the paper is organized as follows: the theoretical background and proposition development are outlined in section 2. Furthermore, we reveal the theoretical facts affecting the bank-fintech collaboration in section 3. In the end, we precisely conclude the issue in section 4.

2. Theoretical background and proposition development

2.1 Potential benefits and detriments of fintech firms

In the last decade, fintech firms promote the European Union policy objective, which is the "capital market union" and the "bank union." These firms serve as a vehicle of value creation for all the ventured business (Milne, 2016). The fintech firms enjoy several advantages due to the technological advancement, like meeting growing customers' demands, faces fewer compliance barriers, better customer experience, effectively streamline the operations, high growth, ease of doing ventures, and innovative business model (Pollari, 2016). The fintech firms have brought breakthroughs in several industries, for example big data (Yin & Gai, 2015), mobile networking (Topol, 2019; Wen et al., 2012; J. Zhang, Chen, Xiang, Zhou, & Xiang, 2012; Y. Zhang & Soong, 2004), mobile embedded systems (Gai, Qiu, Chen, Zhao, & Qiu, 2017; Y. Zhang et al., 2011), trust management (Abawajy, Wang, Yang, & Javadi, 2016; Q. Zhang, Yang, & Chen, 2015), cloud computing (Arcangelo Castiglione et al., 2015; Gai, Qiu, & Zhao, 2018), and image processing (Aniello Castiglione, De Santis, & Soriente, 2007).

Additionally, one of the cutting-edge of fintech firms is the continuous ventures of traditional banks, which have empowered the future of financial institutions. The financial technological advancement facilitates in financial inclusion, broad-ranging applications which are widely accepted, trustworthiness and fairness of financial transactions, new market opportunities to smaller companies, and competitive edge for the venture firms (Medeiros & Chau, 2016). Fintech companies provide smaller innovative start-ups with risk finance. The fintech credit service such as P2P smoothen access to the short-term liquidity for the small and medium enterprises, foster innovative products, and enhance market efficiency (Arner, Barberis, & Buckey, 2016). Dandapani (2017) documents that fintech firms encourage new financial start-ups, which are faster and more cost-effective than their counterparts. Moreover, the fintech firms reduce the public distrust in the traditional finance industry because the financial transactions are rapid, safe, and transparent for the customer (Rooney, Aiken, & Rooney, 2017). The literature entails that fintech firms have a growing trend, and traditional banks bank are relishing the opportunity to collaborate with and learn from these new, innovative businesses.

Nevertheless, the fintech firms come across several issues immediately after the first collaboration with traditional financial institutions. The regulatory requirements for fintech firms are increasing at a rapid rate because of cross-border markets' growing demand and rapidly

transforming the financial system. Milne (2016) indicates that fintech firms are unable to comprehend the banking structure, and it is especially true in terms of regulation and compliance of the banking sector. A recent study claims that although the fintech firms foster the growth of innovative products, yet these firms have a trend to jurisprudence the intellectual property and branding of financial institutions (Medeiros & Chau, 2016). Additionally, Arner et al. (2016) mention that there is no compatible banking infrastructure to support or collaborate with fintech firms. The fintech infrastructure is ineffective due to the system instability, and lack of resilience and security (Pollari, 2016). The alliance of traditional banks and the fintech firms lack innovation as these two parties are reluctant to agree on mutual standards (Teja, 2017). Hence, the literature implies that the fintech firms' infrastructure is incompatible with the traditional banks due to their complex technological business model and regulatory issue.

In conclusion, the previous literature reviews that the fintech firms as the future of the financial sector; however, these firms face several challenges like compliance risk, compatibility issues with a partner firm, every day rapid transformation, and instable technology infrastructure. To our knowledge, there is scarce literature about the cybersecurity issues faced by the traditional banks after the collaboration with the fintech firm. This study makes an attempt to bridge the literature gap of cybersecurity issues of fintech firms and try to determine how fintech firms' collaboration can affect it.

2.2 Cybersecurity risk of fintech firms

Over the past few years, the collaboration between the traditional financial institutions and the fintech firms have enhanced so far. The rationale for collaboration is to improve the quality of the service, agility, innovative mind, and digital infrastructure. Controversy, this alliance enhances the vulnerability of traditional banks to the cybersecurity risk due to inbuild malware attacks, data leakages, and data integrity issues of fintech firms. The fintech firm's cybersecurity risk is a latest fundamental research issue which entails more in-depth analysis to know about different dynamics of emerging cybersecurity issue. The traditional banks amount of vulnerability and fraud exposure increases due to fintech firms' cyber-breach (Ng & Kwok, 2017b). Thus, fintech firms should ensure with the cybersecurity requirements of the respective countries in which they operate.

Lewis & Baker (2013) suggest that the number of cyber-crimes has boosted after the financial inclusion of fintech firms. They also mention that it is difficult to estimate the economic loss faced

by the financial institution because the cyber-attacks affect the operations of financial institutions in different ways. It implies that the cyber-crimes are not only a financial loss for the financial institutions but also a reputational risk for them. Additionally, Kopp et al. (2017) articulate that cyber-breaches lead to loss of the customers, reputation, revenue, brand, equity value, and higher operational costs for fintech firms. The fintech rating agency reports that the cybercrimes can negatively affect the financial performance of the fintech firms as well as the partner firms (Fitch, 2017). Similarly, the International Organization of Securities Commission's Committee on Payments and Market Infrastructures (IOSC-CPMI) and cyber risk expert informs that the cybersecurity risk of fintech firms is relatively higher than the traditional banks. It implies that the cybersecurity issue of fintech firms is a major sustainability concern for partner firms.

Nevertheless, the gravity of fintech cybersecurity risk is very critical for partner financial institutions and the capital market as it can weaken the financial performance of alliance institutions. Although the majority of traditional banks consider fintech partnerships necessary to pursuit profitability opportunities, yet 71% of banks have shown their concerns about the cybersecurity risks supplemented with fintech firms (Digital News Asia, 2018). The cybersecurity concerns by the partner firms especially involve the data integrity risk, data leakage risk, and malware attacks, which are the most significant development inflection points that the partner firms are demanding. Usually, the fintech organizational structure has less capital and human resources. Hence, a lack of resources inhibits fintech firms from spending more on cybersecurity, which threats the sustainability of partner banks.

2.3 Components of cybersecurity risk

In this study, we make efforts to take stock of literature on fintech cybersecurity issues and their consequences on the partner financial institutions. So far, we argue that cybersecurity attacks are escalated after the affiliation with the fintech firms and thereby affecting the financial stability of the banks. The literature also depicts that the business growth and institutional performance are affected by the vulnerability of the fintech cybersecurity system. Among all the institutions, the banking institutions are more fragile to cybersecurity than any other financial institution. Therefore, the industry practitioners and academic researchers share a consensus point of view that the banking institutions' operation risk has a positive association with the financial epidemics of cyber incidences. The fintech expert team and the academics researcher are trying to explore the

reasons why more cyber incidents frequently occur after the fintech partnership with the financial institutions and how to mitigate the gravity of the cyber-attack. In the following literature, we discuss the reasons for fintech cybersecurity.

2.3.1 Malware Attacks

Society for World Interbank Financial Telecommunication (SWIFT) system are usually targeted by hackers globally. Mostly financial institutions used the SWIFT system to secure their financial transfer information. As per the latest cyberattack report of the second largest bank in India, the hackers demonstrated a high level of sophistication in recent malware attacks on the SWIFT system. Hence after the banks venture into fintech partnerships, but the vulnerability of malware attacks has been increased in recent years. A recent survey report of SWIFT indicates that the hackers take advantage of the fintech vulnerabilities and try to choose only those banks which have set up a regulatory sandbox with the fintech firms (Vimal, 2019). Research indicates that hackers are targeting more fintech firms and their partner's firms due to the vulnerability of cybersecurity (Austin & Bloggs, 2018). According to McAfee expert opinion, the cumulative number of malware attacks will be exceeded by 700 million by the end of 2020 (McAfee, 2019). It implies that traditional banks become the target of the hackers immediately after the joint venture with fintech firms as the fintech firms have weak cybersecurity.

2.3.2 Data Leakages

Besides the malware attacks, another cybersecurity issue faced by banks is data leakage. It is documented that after the partnership with fintech firms, the number of data leakage attacks has been increased so far (Ozili, 2018). Financial data includes user credentials and payment card information. Data leakage is a perennial and common issue faced by fintech firms. Seemingly, the fintech service providers are relatively more vulnerable to data leakage than other financial institutions (Yalcin, 2018) as all the services are digitals. After the banks venture with fintech companies, then they have to provide customers' valuable information to fintech service providers; however, the fintech firms are particularly exposed to sensitive data leaks (Vimal, 2019). Also, cloud computing is one of the cutting edges of the fintech ecosystem, but a lack of suitable cloud measures will lead to data leakage. In conclusion, recent literature indicates that fintech firms are susceptible to financial data leakage, which ultimately results in cybersecurity risk.

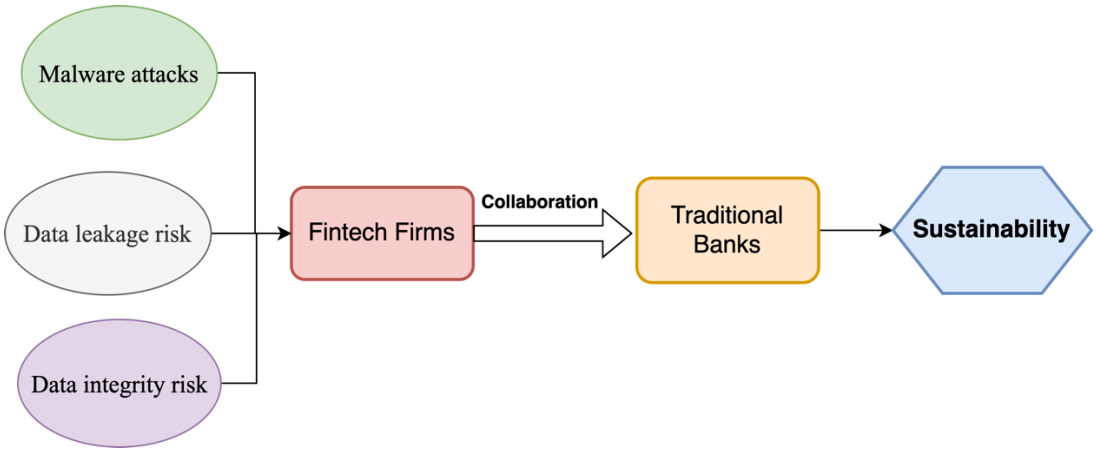
2.3.3 Data Integrity Risk

Mobile internet banking plays a significant role in collaboration with fintech services. The mobile device needs to have a robust compactable encryption system to support the fintech services; otherwise, data integrity risk will rise. Recent research finds that the integrity of data varies dramatically from one mobile money application to another (Subashini & Kavitha, 2011). Another major enabler of the fintech ecosystem is cloud computing. It includes digital wallets, payment gateways, and online payments. Although it is effortless and fast to make online payment through cloud computing, still maintaining secure and confidential financial information is an uphill task for the fintech firms. A sophisticated cloud security measures are required for the robust encryption mechanism of this sensitive information. Additionally, the integrity of data gathered from the fintech applications seems skeptical and varied dramatically across different sample sets (Anton-Diaz, 2018). In a nutshell, data integrity issues ultimately lead to cybersecurity risk for fintech firms.

After reviewing the literature of fintech firms' data integrity risk, data leakage risk, and malware attacks, we conjecture that the fintech firms are vulnerable to cybersecurity risk. Also, immediately after the collaboration with the banking institutions, the inherent cybersecurity risk of fintech firms becomes the value-demolishing factor for banks. Hence, the fintech and banks alliances raise questions for the sustainability of banks. The theoretical framework of the study is as follows:

Figure I

Theorical Framework



Until now, we discuss the fintech cybersecurity risk and possible causes of it, which come across three thematic areas such as data integrity risk, data leakage risk, and malware attacks. The traditional banks and fintech firms agree that they need one another; however, this alliance exacerbates the cybersecurity vulnerabilities for banks due to the inherent cybersecurity issues of fintech. Therefore, the technical dependency of traditional banks results in facing cyber-attacks.

Following the above premises, the hypothesis of the study is as follows:

> *P_1: The traditional bank's cybersecurity risk increases after the collaboration with the fintech firm.*

3. Theorical facts revealing the impact of fintech collaboration on banks

The business model and firm structure of the fintech firms are more vulnerable to cybersecurity shocks as compared to the other financial institutions (Ng & Kwok, 2017a). The trickle-down effect of these shocks on the fintech firms will spread to the other partner industrial sectors, which are availing the fintech services. The concern about the vulnerability of fintech firm's business model stem from the digitalization. A cyberattack on fintech firms can cause a loss of confidential data, and these attacks can expose to other sectors related to the fintech firms. Therefore, the market information about the operations and structure of the fintech firm cannot be reliable. These problems suggest that the fintech firms offer a set of cybersecurity and regulatory issues that are more severe than other financial institutions.

Despite the various benefits linked with the fintech firms, one may undermine the issues arising from these emerging financial technology solutions. Treleaven (2015) suggests that since the fintech firms do business operations under digitization, therefore fintech firms are more vulnerable to cyberattacks than the other financial institutions. When a cybercrime takes place within the fintech setup, then it is difficult to identify because of the absence of a monitoring body (Kwok, 2017). According to the recent survey by an antivirus firm, the financial sector is 300 times more vulnerable to cyberattacks than any other industrial sector (Market Insider, 2019). The high level of vulnerability is because 81% of the financial sector outsource their financial technology services via fintech firms, which also results in high data leakage costs for financial institutions (Yalcin, 2018).

Financial technological development enhances the likelihood of cyber incidents worldwide. After the third-party collaboration of the fintech firms with the financial sectors, we find that the cybercrimes are taking place more frequently as compared to the prior years. Those financial institutions which avail the fintech service are galloping target for the hackers. In addition, to suppose this argument, we can refer to a set of recent cyberattacks that take place across the world in the last few years.

In recent years, the number of cyber-attacks reported by financial institutions is increasing at a rapid rate. Table 1 shows that after the fintech revolution, the number of cybercrimes reported has been increased. JP Morgan Chase was the first in the list to collaborate with the fintech firms in 2014. Within a few months of collaboration, the bank faced USD 76 million loss due to the hacking activity. It was the biggest hacking reported at that time (The New York Times, 2014). Afterward, Central Coast Credit Union became alliance with fintech firms on 13th April 2016. The financial institution reported a cyber-attack within one year of collaboration, which resulted in a USD 60,000 loss (Kreb on Security, 2016). In the same year, Capital One collaborates with the fintech firms and introduce the fintech sandbox. However, the cybersecurity of Capital One compromised from the three years of fintech collaboration, and the online banking system hacked on 4th November 2019, which leads to USD 106 million loss for the institution (Capital One, 2019). On 11th June 2019, Desjardins partners with fintech firms, and in the same year, the institution report a cybersecurity breach resulting in USD 2.90 million loss (CBC, 2019). Again, Westpac financial institution initiated the fintech sandbox service on 7th November 2019, and within two months of service, the online bank system hacked, causing USD 98,000 financial loss, and almost 100,000 customers sensitive information was exposed (Finance Nine, 2019). In the last, First American Corporation lost USD 885 million from the poor cybersecurity, whereas this institution collaborated with the fintech firm on 27th November 2018 (Gizmodo, 2019).

Table 1: The list of cyber-attacks of fintech partner banks.

Equity	Date of Collaboration with Fintech	Year of cyber-crime	Amount Lost (USD)	Sector	Reported Reason
JP Morgan Chase	3rd- Apr-14	2014	76,000,000	financial	Hacked
Central Coast Credit Union	13-Apr-16	2016	60,000	financial	Hacked
Capital One	4-Nov-16	2019	106,000,000	financial	Hacked
Desjardins	11-Jun-19	2019	2,900,000	financial	Inside job
Westpac	7-Nov-19	2019	98,000	financial	Hacked
First American Corporation	27-Nov-18	2019	885,000,000	financial service company	Poor cyber-security

Source: The above information is gathered from Wikipedia (2020).

These cyber-attacks indicate that the banks face more cyber-attacks after the alliance with the fintech firms. The duration of the collaboration with fintech firms is insignificant as few banks hacked within a couple of months of partnership, and some banks reported cyber-crime more than two years (for example, Capital One).

The above cybercrimes are only those attacks that are reported by the banks; however, there are many cyber-attacks that are not documented due to the banks' reputation and the gravity of the situation. Nevertheless, these incidents indicate a clear cybersecurity risk associated with fintech firms negatively impact the partner banks. The cybersecurity risk not only cases the significant financial loss but also erode the investor's confidence in the fintech firms and their partner firms (financial institutions). Also, the financial institutions are contributing a significant part of the gross domestic production (GDP) worldwide. Hence cybersecurity risk is not merely a technical issue of the fintech firm or its partner firms, and it may also cause financial instability across the world, and based on these cyber-attacks, we can observe the consequence of fintech cybersecurity lapse for partner financial institutions.

4. Conclusion

This article shed light on the fintech firms' implications for financial institutions and financial inclusion, and its inherent risk of cybersecurity. Collaboration with fintech firms has many advantages like operational cost-saving, low cost for customers, and faster service. Despite the advantage of fintech firms, this article emphasizes some challenges faced by fintech firms along with its partner firms. As every year passing, the rate of cybercrimes has been increased so far. Additionally, cybersecurity is the primary concern for fintech firms due to which in recent years, the traditional banks taking service of fintech firms are more vulnerable to cyberattacks. One of the possible reasons for higher cybersecurity incidents is the compatibility issues of fintech firms' services with the financial institutions, the operation size of financial institutions is bigger for the fintech firms to handle it. The theoretical evidence shows that the immediate after the fintech collaboration, the financial institutions report cyber-attacks issues. This happens because the fintech firms transfer their inherent cyber-risk to the partner financial institutions.

The present study has a number of limitations that should be addressed by future research. First, the financial institutions do not disclose all the cybersecurity issues and kept privately, which is difficult to access. Second, future research tries to examine the impact of cybersecurity issue of fintech on the stability of fintech partner banks. Third, future research can extend this study by using a systematic econometric model such as ordinary least squares model or probit model.

Reference

Abawajy, J., Wang, G., Yang, L. T., & Javadi, B. (2016). Trust, security and privacy in emerging distributed systems FGCS. *Future Generation Computer Systems*, *55*, 224–226.

Anton-Diaz, P. (2018). New Data Security Study of Fintech Apps Highlights Vulnerabilities | Center for Financial Inclusion. Retrieved April 4, 2020, from New Data Security Study of Fintech Apps Highlights Vulnerabilities," Center for Financial Inclusion, 5 September 2018 website: https://www.centerforfinancialinclusion.org/new-data-security-study-of-fintech-apps-highlights-vulnerabilities

Arakji, R. Y., & Lang, K. R. (2007). Digital consumer networks and producer-consumer collaboration: innovation and product development in the video game industry. *Journal of Management Information Systems*, *24*(2), 195–219.

Arner, D. W., Barberis, J., & Buckey, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. *Nw. J. Int'l L. & Bus.*, *37*, 371.

Austin, J., & Bloggs, J. (2018). Big Data Outsourcing and Identity Verification in Fintech Credit Assessment: A Case Study of a Microloans Platform in China. *Australasian Conference on Information Systems*.

Buckley, R. P., Arner, D. W., Zetzsche, D. A., & Selga, E. (2019). The Dark Side of Digital Financial Transformation: The New Risks of FinTech and the Rise of TechRisk. *UNSW Law Research Paper*, (19–89).

Capital One. (2019). 2019 Capital One Cyber Incident | What Happened | Capital One. Retrieved May 1, 2020, from https://www.capitalone.com/facts2019/

Castiglione, Aniello, De Santis, A., & Soriente, C. (2007). Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. *Journal of Systems and Software*, *80*(5), 750–764.

Castiglione, Arcangelo, Pizzolante, R., De Santis, A., Carpentieri, B., Castiglione, A., & Palmieri, F. (2015). Cloud-based adaptive compression and secure management services for 3D healthcare data. *Future Generation Computer Systems*, *43*, 120–134.

CBC. (2019). Personal data of 2.7 million people leaked from Desjardins | CBC News. Retrieved May 1, 2020, from https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297

Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime*.

Dandapani, K. (2017). Electronic finance–recent developments. *Managerial Finance*.

Digital News Asia. (2018). Cyber-security the biggest barrier to fintech and banking sector partnerships in Asia | Digital News Asia. Retrieved April 7, 2020, from

https://www.digitalnewsasia.com/digital-economy/cyber-security-biggest-barrier-fintech-and-banking-sector-partnerships-asia

Finance Nine. (2019). Westpac security breach: Almost 100,000 customers exposed, cyber security news update. Retrieved May 1, 2020, from https://finance.nine.com.au/business-news/westpac-data-breach-100000-australian-customers-at-risk/84c91581-90b6-464e-9137-a2d973492614

Fitch. (2017). [Press Release] Fitch: Cyber Risk Is a Growing Threat to Financial Institutions. Retrieved January 31, 2020, from https://www.fitchratings.com/site/pr/1022468

Gai, K., Qiu, L., Chen, M., Zhao, H., & Qiu, M. (2017). SA-EAST: security-aware efficient data transmission for ITS in mobile heterogeneous cloud computing. *ACM Transactions on Embedded Computing Systems (TECS)*, *16*(2), 1–22.

Gai, K., Qiu, M., & Zhao, H. (2018). Energy-aware task assignment for mobile cyber-enabled applications in heterogeneous cloud computing. *Journal of Parallel and Distributed Computing*, *111*, 126–135.

Gizmodo. (2019). 885 Million Records Exposed Online: Bank Transactions, Social Security Numbers, and More. Retrieved May 1, 2020, from https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235

Haupert, V., Maier, D., & Tilo, M. (2017). Paying the Price for Disruption: How a FinTech Allowed Account Takeover. https://doi.org/https://doi.org/10.1145/3150376.3150383

Kopp, E., Kaffenberger, L., & Jenkinson, N. (2017). *Cyber risk, market failures, and financial stability*. International Monetary Fund.

Kreb on Security. (2016). Breached Credit Union Comes Out of its Shell — Krebs on Security. Retrieved May 1, 2020, from https://krebsonsecurity.com/2016/02/breached-credit-union-comes-out-of-its-shell/

Kwok, B. K. B. (2017). *Accounting irregularities in financial statements: A definitive guide for litigators, auditors and fraud investigators*. Routledge.

Lewis, J., & Baker, S. (2013). *The economic impact of cybercrime and cyber espionage*. McAfee.

Market Insider. (2019). Cyberattacks are 300 times as likely to hit financial firms than other companies. A sweeping new report finds they're not prepared. | Markets Insider. Retrieved February 1, 2020, from https://markets.businessinsider.com/news/stocks/cyberattacks-impact-major-threats-to-financial-firms-not-prepared-2019-6-1028296130

McAfee. (2019). *McAfee Labs Threats Report New Ransomware Techniques Discovered High-Profile Data Dumps Expose Billions of Accounts Attackers Target More Lucrative Returns from Larger Enterprises*.

McAfee. (2020). Study: $100 Billion Lost Annually to Cyber Attacks | 2013-07-22 | Security

Magazine. Retrieved April 24, 2020, from https://www.securitymagazine.com/articles/84549-study-100-billion-lost-annually-to-cyber-attacks

Medeiros, M., & Chau, B. (2016). Fintech-Stake a Patent Claim? *Intellectual Property Journal*, *28*(3), 303.

Milne, A. (2016). Competition policy and the financial technology revolution in banking. *Communications & Strategies*, *103*, 145–161.

Mok, A., & Saha, R. (2017). Strategic risk management in banking. *Deloitte Inside Magazine*.

Ng, A. W., & Kwok, B. K. B. (2017a). Emergence of Fintech and cybersecurity in a global financial centre: Strategic approach by a regulator. *Journal of Financial Regulation and Compliance*, *25*(4), 422–434. https://doi.org/10.1108/JFRC-01-2017-0013

Ng, A. W., & Kwok, B. K. B. (2017b). Emergence of Fintech and cybersecurity in a global financial centre. *Journal of Financial Regulation and Compliance*.

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329–340.

Pollari, I. (2016). The rise of Fintech opportunities and challenges. *Jassa*, (3), 15.

Rooney, H., Aiken, B., & Rooney, M. (2017). Q. Is Internal Audit Ready for Blockchain? *Technology Innovation Management Review*, *7*(10), 41–44.

Sajtos, P. F. P., & Tőrös, Á. (2018). Regulatory Tools to Encourage FinTech Innovations: The Innovation Hub and Regulatory Sandbox in International Practice. *Financial and Economic Review*, 43.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, *34*(1), 1–11.

Teja, A. (2017). Indonesian FinTech business: New innovations or foster and collaborate in business ecosystems? *The Asian Journal of Technology Management*, *10*(1), 10.

The New York Times. (2014). JPMorgan Chase Hacking Affects 76 Million Households - The New York Times. Retrieved May 1, 2020, from https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/?_php=true&_type=blogs&_r=0

Topol, E. J. (2019). High-performance medicine: the convergence of human and artificial intelligence. *Nature Medicine*, *25*(1), 44–56.

Treleaven, P. (2015). Financial regulation of FinTech. *Journal of Financial Perspectives*, *3*(3).

Vimal, M. (2019). Cybersecurity and Fintech at a Crossroads. Retrieved April 7, 2020, from

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/cybersecurity-and-fintech-at-a-crossroads

Wen, S., Zhou, W., Zhang, J., Xiang, Y., Zhou, W., & Jia, W. (2012). Modeling propagation dynamics of social network worms. *IEEE Transactions on Parallel and Distributed Systems*, *24*(8), 1633–1643.

Wikipedia. (2020). List of data breaches - Wikipedia. Retrieved May 1, 2020, from https://en.wikipedia.org/wiki/List_of_data_breaches#cite_note-65

Yalcin, F. G. (2018). Finans Sektörü 300 Kat Daha Fazla Saldırıya Uğruyor | Fintechtime. Retrieved January 26, 2020, from http://fintechtime.com/tr/2018/10/finans-sektoru-300-kat-daha-fazla-saldiriya-ugruyor/

Yin, H., & Gai, K. (2015). An empirical study on preprocessing high-dimensional class-imbalanced data for classification. *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, 1314–1319. IEEE.

Zhang, J., Chen, C., Xiang, Y., Zhou, W., & Xiang, Y. (2012). Internet traffic classification by aggregating correlated naive bayes predictions. *IEEE Transactions on Information Forensics and Security*, *8*(1), 5–15.

Zhang, Q., Yang, L. T., & Chen, Z. (2015). Privacy preserving deep computation model on cloud for big data feature learning. *IEEE Transactions on Computers*, *65*(5), 1351–1362.

Zhang, Y., & Soong, B.-H. (2004). Performance evaluation of GSM/GPRS networks with channel re-allocation scheme. *IEEE Communications Letters*, *8*(5), 280–282.

Zhang, Y., Yu, R., Xie, S., Yao, W., Xiao, Y., & Guizani, M. (2011). Home M2M networks: architectures, standards, and QoS improvement. *IEEE Communications Magazine*, *49*(4), 44–52.